IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF ALABAMA
SOUTHERN DIVISION

MARY FRANCES JONES, individually and on behalf of all others similarly situated,

Plaintiff,

v.

COMMUNITY HEALTH SYSTEMS, INC., COMMUNITY HEALTH SYSTEMS PROFESSIONAL SERVICES CORPORATION, TRIAD OF ALABAMA, LLC

Defendants.

Case No.: 1:15-CV-201

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Mary Frances Jones, on behalf of herself and all others similarly situated, by and through his attorneys, bring this action against Community Health Systems, Inc., Community Health Systems Professional Services Corporation and Triad of Alabama, LLC (collectively "CHS" or "Defendants"), and hereby alleges as follows:

NATURE OF THE CASE

1. This is a consumer class action lawsuit brought by Plaintiff, individually and on behalf of all other similarly situated persons (i.e., the Class Members), whose personally identifiable information and personal health

information— names, addresses, dates of birth, Social Security numbers, treating physician and/or departments for each individual, their medical diagnoses, medical record numbers, medical service codes, and health insurance information (collectively referred to as "PII/PHI")— entrusted to CHS was stolen by and/or made accessible to a thief or computer hackers while in the possession, custody, and control of CHS.

2. Through information and belief, from approximately April, 2014 through June, 2014, data containing the PII/PHI of Plaintiff and millions of other Class Members was left unguarded, unprotected, unencrypted and/or otherwise subject to theft by third parties who otherwise had no reason to be in possession of such information. As a result, the PII/PHI of thousands of Class Members was stolen as a result of a data breach of CHS. (the "Data Breach").

3. CHS flagrantly disregarded Plaintiff's and the other Class Members' privacy rights by intentionally, willfully, recklessly, negligently and/or wantonly failing to take the necessary precautions required to safeguard and protect their PII/PHI from unauthorized disclosure or dissemination. Plaintiff's and Class Members' PII/PHI was improperly handled and stored, and was otherwise not kept in accordance with applicable and appropriate security protocols, policies and procedures. As a result, Plaintiff's and Class Members' PII/PHI was compromised and/or stolen.

4. CHS's intentional, willful, reckless, negligent and/or wanton disregard of Plaintiff's and Class Members' rights directly and/or proximately caused a substantial unauthorized disclosure of Plaintiff's and Class Members' PII/PHI. The improper use of PII/PHI by unauthorized third parties can result in an adverse impact on, among other things, a victim's credit rating and finances. The type of wrongful PII/PHI disclosure made by CHS is the most harmful because it generally takes a significant amount of time for a victim to become aware of misuse of that PII/PHI.

5. On behalf of herself and Class Members, Plaintiff has standing to bring this lawsuit because she suffered actual damages as a direct and/or proximate result of CHS's wrongful actions and/or inaction and the resulting Data Breach.

6. CHS's wrongful actions and/or inaction and the resulting Data Breach have placed Plaintiff and Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[1] Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released a 2012 Identity Fraud Report (the "Javelin Report") quantifying the impact of data breaches. According to the Javelin

[1] According to the United States Government Accounting Office, the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities, such as when PII/PHI is used to commit fraud or other crimes (credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services)).

Report, individuals whose PII/PHI is subject to a reported data breach— such as the Data Breach at issue here— are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity theft and/or identity fraud has not yet been discovered or reported and a high probability that criminals who may now possess Plaintiff's and Class Members' PII/PHI have not yet used the information but will do so later, or re-sell it. Even without such loss, Plaintiff and Class Members are entitled to relief and recovery, including statutory damages under federal statutory provisions as set forth herein.

7. CHS's failure to safeguard and secure Plaintiff's and Class Members' PII/PHI violated the Fair Credit Reporting Act, 15 U.S.C. § 1681 et. seq. ("FCRA"). CHS failed to adopt, implement, and/or maintain adequate procedures to protect such information and limit its dissemination to the permissible purposes under FCRA. In further violation of FCRA, CHS failed to protect and wrongfully disseminated Plaintiff's and Class Members' PII/PHI, which is "medical information" specifically defined in, and protected by, FCRA. As a direct and/or proximate result of CHS's willful, reckless and/or grossly negligent violations of FCRA, an unauthorized third party (or parties) obtained Plaintiff's and Class Members' PII/PHI for no permissible purpose under FCRA.

8. CHS's wrongful actions and/or inaction also constitute common law negligence and common law invasion of privacy by public disclosure of private facts. Further, CHS's wrongful actions and/or inaction constitutes a breach of contract.

9. Plaintiff, on behalf of herself and the Class Members, seek actual damages, economic damages, statutory damages, nominal damages, exemplary damages, injunctive relief, attorneys' fees, litigation expenses and costs of suit.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over Plaintiff's FCRA claims pursuant to 28 U.S.C. § 1331 (federal question). This Court also has subject matter jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367. Finally, this Court has subject matter jurisdiction based upon diversity jurisdiction under the Class Action Fairness Act ("CAFA"), . This Court has personal jurisdiction over CHS because, at all relevant times, CHS conducted (and continues to conduct) substantial business in the Middle District of Alabama.

11. Venue is proper in the Middle District of Alabama pursuant to 28 U.S.C. §1391(b) and (c) because a substantial part, if not all, of the events giving rise to this action occurred in the Middle District of Alabama and CHS owned hospitals are located, can be found, and/or conduct substantial business in the

Middle District of Alabama.

PARTIES

12. Plaintiff Mary Frances Jones is an Alabama citizen residing in the Houston County located in the Middle District of Alabama. Plaintiff was treated at Flowers Hospital, a hospital owned by or affiliated with CHS, during the relevant time period, and, through information and belief, his PII/PHI was subjected to the aforementioned Data Breach. Recently, Plaintiff was informed by CHS that her PII/PHI had been subject to the Data Breach.

13. Through information and belief, Plaintiff's PII/PHI, which she entrusted to CHS and which CHS failed to properly safeguard, was stolen from CHS as part of the Data Breach.

14. As a direct and/or proximate result of CHS's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff has suffered economic damages relating to the theft of her Social Security number and PII/PHI, and other actual harm, including but not limited to emotional distress over learning of the theft of her PII/PHI. CHS's wrongful disclosure of and failure to safeguard Plaintiff's PII/PHI has also placed her at an imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud, and medical fraud.

15. Defendant, Community Health Systems, Inc., is a Delaware corporation with its principal place of business in Tennessee. Upon information

and belief, Community Health Systems, Inc. was doing business in the Middle District of Alabama at all times materially relevant hereto. Further, upon information and belief, Community Health Systems, Inc. owns or operates, through subsidiaries, over 200 hospitals in the United States, including Triad of Alabama, LLC d/b/a Flowers Hospital in Dothan, Alabama.

16. Defendant, Community Health Systems Professional Services Corporation, is a Delaware corporation with its principal place of business in Tennessee. Upon information and belief, Community Health Systems Professional Services Corporation does business in Alabama.

17. Defendant, Triad of Alabama, LLC d/b/a Flowers Hospital ("Flowers") is a health care entity qualified to do business in Alabama and was doing business in the Middle District of Alabama at all times materially relevant hereto.

BACKGROUND FACTS

18. In the regular course of its business, CHS, through its hospitals, collects and maintains possession, custody, and control of a wide variety of Plaintiff's and Class Members' personal and confidential information, including: names, addresses, dates of birth, Social Security numbers, treating physician and/or departments for each individual, their medical diagnoses, medical record numbers, medical service codes, and health insurance information (collectively

referred to as "PII/PHI").

19. CHS stored Plaintiff's and Class Members' PII/PHI, at a minimum, in an unprotected, unguarded, unsecured, and/or otherwise unreasonable location upon its premises or its servers. Plaintiff's and Class Members' PII/PHI was not encrypted.

20. Plaintiff's and Class Members' PII/PHI was stored in such a manner that it had little or no security to prevent unauthorized access.

21. Plaintiff reasonably believes that the number of Class Members whose PII/PHI was stolen in the Data Breach exceeds one million.

22. Plaintiff's and Class Members' PII/PHI could have been bought and sold several times on the robust international cyber black market. Meanwhile, Plaintiff and Class Members had no chance whatsoever to take measures to protect their privacy.

23. CHS's wrongful actions and/or inaction— to wit, failing to protect Plaintiff's and Class Members' PII/PHI with which it was entrusted— directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII/PHI without their knowledge, authorization, and/or consent. As a further direct and/or proximate result of CHS's wrongful actions and/or inaction, Plaintiff and Class Members have suffered, and will continue to suffer, damages including, without limitation: (i) the untimely and/or

inadequate notification of the Data Breach; (ii) improper disclosure of their PII/PHI; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (v) economic losses relating to the theft of their Social Security numbers; (vi) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vii) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (viii) anxiety and emotional distress; and (ix) rights they possess under FCRA— for which they are entitled to compensation.

24. Notwithstanding CHS's wrongful actions and/or inaction, CHS has offered a mere one year of credit monitoring services, which is insufficient, given the trove of unencrypted PII/PHI that has been taken and disseminated to the world.

25. As a result of CHS's failure to properly safeguard and protect Plaintiff's and Class Members' PII/PHI, Plaintiff's and Class Members' privacy has been invaded and their rights violated. Their compromised PII/PHI was private and sensitive in nature and was left inadequately protected by CHS. CHS's wrongful actions and/or inaction and the resulting Data Breach have placed Plaintiff and Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.

26. Identity theft occurs when a person's PII, such as the person's name, e-mail address, address, Social Security number, billing and shipping addresses, phone number and credit card information is used without his or her permission to commit fraud or other crimes.[2]

27. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[3] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute [PII]."[4]

28. The FTC estimates that the identities of as many as 9 million Americans are stolen each year. *Id.*

29. As a direct and/or proximate result of the Data Breach, Plaintiff and

---

[2] See http://www.consumer.ftc.gov/features/feature-0014-identity-theft (last visited Aug. 29, 2013).

[3] Protecting Consumer Privacy in an Era of Rapid Change FTC Report (March 2012) (http://www.ftc.gov/os/2012/03/120326privacyreport.pdf) (last visited Aug. 29, 2013).

[4] Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report, 35–38 (Dec. 2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (last visited Aug. 29, 2013); Comment of Center for Democracy & Technology, cmt. #00469, at 3; Comment of Statz, Inc., cmt. #00377, at 11–12.

Class Members will now be required to spend money and to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, placing "freezes" and "alerts" with the credit reporting agencies, closing or modifying financial accounts, scrutinizing their bank and credit accounts and purchasing products to monitor their credit reports and accounts for unauthorized activity. Because Plaintiff's and Class Members' Social Security numbers were stolen and/or compromised, they also now face a significantly heightened risk of identity theft.

30. According to the FTC, identity theft is serious. "Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest."[5]

31. Theft of medical information, such as that included in the Data Breach here, is equally serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be

[5] *See* Federal Trade Commission, *Signs of Identity Theft*, http://www.consumer.ftc.gov/articles/0271- signs-identity-theft (last visited Aug. 29, 2013).

affected."[6]

32. Identity thieves also use Social Security numbers to commit other types of fraud. The GAO found that identity thieves use PII/PHI to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, while in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PII/PHI, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future.

33. Identity thieves also use Social Security numbers to commit other types of fraud, such as obtaining false identification cards, obtaining government benefits in the victim's name, committing crimes and/or filing fraudulent tax returns on the victim's behalf to obtain fraudulent tax refunds. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments, and/or obtain medical services in the victim's name. Identity thieves also have been known to give a victim's personal information to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as

[6] See Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171- medical-identity-theft (last visited Aug. 29, 2013).

well the damage to their "good name."

34. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently, as well as show that she has done all she can to fix the problems resulting from the misuse.[7] Thus, a person whose PII/PHI has been stolen cannot obtain a new Social Security number until the damage has already been done.

35. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems. Because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

36. As a direct and/or proximate result of CHS's wrongful actions and/or inaction and the Data Breach, the thieves and/or their customers now have Plaintiff's and Class Members' PII/PHI. As such, Plaintiff and Class Members

[7] See Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327 (http://www.ssa.gov/pubs/10064.html) (last visited Aug. 29, 2013).

have been deprived of the value of their PII/PHI.[8]

37. Plaintiff's and Class Members' PII/PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for a number of years.[9] Identity thieves and other cyber criminals openly post stolen credit card numbers, Social Security numbers, and other personal financial information on various Internet websites, thereby making the information publicly available. In one study, researchers found hundreds of websites displaying stolen personal financial information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism the "Safe Browsing list." The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your

---

[8] *See, e.g.*, John T. Soma, J. Zachary Courson, John Cadkin, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted); ABC News Report, http://abcnews.go.com/Health/medical-records-private-abc-news-investigation/story?id=17228986&page=2#.UGRgtq7yBR4 (last visited Aug. 29, 2013).

[9] Companies, in fact, also recognize PII/PHI as an extremely valuable commodity akin to a form of personal property. See T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

face."[10]

38. The Data Breach was a direct and/or proximate result of CHS's failure to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect Plaintiff's and Class Members' PII/PHI from unauthorized access, use, and/or disclosure, as required by various state regulations and industry practices.

39. CHS flagrantly disregarded and/or violated Plaintiff's and Class Members' privacy rights, and harmed them in the process, by not obtaining Plaintiff's and Class Members' prior written consent to disclose their PII/PHI to any other person— as required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and other pertinent laws, regulations, industry standards and/or internal company standards.

40. CHS flagrantly disregarded and/or violated Plaintiff's and Class Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII/PHI to protect against anticipated threats to the security or integrity of such information. CHS's security deficiencies allowed unauthorized

[10] StopTheHacker, The "Underground Credit Card Blackmarket," http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/ (last visited Aug. 29, 2013).

individuals to access, remove from its premises, transport, disclose, and/or compromise the PII/PHI of thousands of individuals— including Plaintiff and Class Members.

41. CHS's wrongful actions and/or inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII/PHI without their knowledge, authorization, and consent. As a direct and proximate result of CHS's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and Class Members have incurred damages in the form of, *inter alia*: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure of their PII/PHI; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under FCRA— for which they are entitled to compensation.

CLASS ACTION ALLEGATIONS

42. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this class action as a national class action on behalf of herself and

the following Class of similarly situated individuals:

> All persons whose personal identifying information (PII) and personal health information (PHI) was stolen and/or exposed to potential theft from CHS between April 1, 2014 and July 31, 2014.

Excluded from the Class are the (i) owners, officers, directors, employees, agents and/or representatives of Defendants and their parent entities, subsidiaries, affiliates, successors, and/or or assigns, and (ii) the Court, Court personnel, and members of their immediate families.

43. The putative Class is, through information and belief, comprised of tens of thousands, making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

44. The rights of each Class Member were violated in a virtually identical manner as a result of CHS's willful, reckless, and/or negligent actions and/or inaction.

45. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, inter alia:

a) Whether CHS violated FCRA by failing to properly secure Plaintiff's and Class Members' PII/PHI;

b) Whether CHS willfully, recklessly, and/or negligently failed to

maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class Members' PII/PHI;

c) Whether CHS was negligent in the manner in which it stored Plaintiff's and Class Members' PII/PHI;

d) Whether CHS owed a duty to Plaintiff and Class Members to exercise reasonable care in protecting and securing their PII/PHI;

e) Whether CHS breached its duty to exercise reasonable care in protecting and securing Plaintiff's and Class Members' PII/PHI;

f) Whether CHS was negligent in failing to secure Plaintiff's and Class Members' PII/PHI;

g) Whether CHS's failure to comply with HIPAA constitutes negligence *per se*;

h) Whether CHS breached its contracts by failing to maintain the privacy and security of Plaintiff's and Class Members' PII/PHI;

i) Whether by publicly disclosing Plaintiff's and Class Members' PII/PHI without authorization, CHS invaded Plaintiff's and Class Members' privacy; and

j) Whether Plaintiff and Class Members sustained damages as a result of CHS's failure to secure and protect their PII/PHI.

46. Plaintiff's claims are typical of Class Members' claims in that

Plaintiff's claims and Class Members' claims all arise from CHS's failure to properly secure and protect Plaintiff's and Class Members' PII/PHI and the resulting Data Breach.

47. Plaintiff and his counsel will fairly and adequately represent the interests of Class Members. Plaintiff has no interests antagonistic to, or in conflict with, Class Members' interests. Plaintiff's lawyers are experienced litigators and intend to vigorously prosecute this action on behalf of Plaintiff and Class Members.

48. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiff's and Class Members' claims. Plaintiff and Class Members have been irreparably harmed as a result of CHS's wrongful actions and/or inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to CHS's failure to secure and protect Plaintiff's and Class Members' PII/PHI.

49. Class certification, therefore, is appropriate pursuant to FED.R.CIV.P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

50. Class certification also is appropriate pursuant to FED.R.CIV.P.

23(b)(2) because Defendants have acted or refused to act on grounds generally applicable to the class, thereby making final injunctive relief appropriate with respect to the class as a whole.

51. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights.

CLAIMS FOR RELIEF/CAUSES OF ACTION

COUNT I
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

52. The preceding factual statements and allegations are incorporated by reference.

53. The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to adopt and maintain procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. 15 U.S.C. § 1681(b).

54. FCRA defines a "consumer reporting agency" as:

> Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties,

and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. 15 U.S.C. § 1681a(f).

FCRA defines a "consumer report" as:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b). 15 U.S.C. § 1681a(d)(1).

55. FCRA defines "medical information" as:

> [I]nformation or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to--(A) the past, present, or future physical, mental, or behavioral health or condition of an individual; (B) the provision of health care to an individual; or (C) the payment for the provision of health care to an individual. 15 U.S.C. § 1681a(i).

56. FCRA specifically protects medical information, restricting its dissemination to limited instances. See, e.g., 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681c(a)(6).

57. CHS is a Consumer Reporting Agency as defined under FCRA because on a cooperative nonprofit basis and/or for monetary fees, CHS regularly engages, in whole or in part, in the practice of assembling information on

consumers for the purpose of furnishing Consumer Reports to third parties and/or uses interstate commerce for the purpose of preparing and/or furnishing Consumer Reports.

58. As a Consumer Reporting Agency, CHS was (and continues to be) required to adopt and maintain procedures designed to protect and limit the dissemination of consumer credit, personnel, insurance and other information (such as Plaintiff's and Class Members' PII/PHI) in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. CHS, however, violated FCRA by failing to adopt and maintain such protective procedures which, in turn, directly and/or proximately resulted in the theft of Plaintiff's and Class Members' PII/PHI and its wrongful dissemination into the public domain. By way of example, CHS could have:

a) Conducted periodic risk assessments and gap analysis relating to privacy and information security-related policies, processes and procedures. A comprehensive risk analysis would have identified the (i) physical vulnerability of CHS's file locations, and (ii) administrative vulnerabilities associated with storing files containing patients' PII/PHI in an unsecured and unencrypted manner.

b) Developed privacy and information security related performance and

activity metrics, such as the performance of ongoing compliance reviews, physical walkthroughs (roundings), hotline and complaint management— and ensure that these metrics were an integral part of CHS's corporate governance program.

c) Taken measures to monitor and secure the data servers and areas where the files containing the PII/PHI were stored, maintained, and used, or taken measures to insure that no PII/PHI was stored in unsecured, unencrypted, and/or unguarded locations.

On information and belief, CHS took none of these proactive actions to secure and protect Plaintiff's and Class Members' PII/PHI.

59. Plaintiff's and Class Members' PII/PHI, in whole or in part, constitutes medical information as defined by FCRA. CHS violated FCRA by failing to specifically protect and limit the dissemination of Plaintiff's and Class Members' PII/PHI (i.e., their medical information) into the public domain.

60. As a direct and/or proximate result of CHS's willful and/or reckless violations of FCRA, as described above, Plaintiff's and Class Members' PII/PHI was stolen and/or made accessible to unauthorized third parties in the public domain.

61. As a direct and/or proximate result of CHS's willful and/or reckless

violations of FCRA, as described above, Plaintiff and Class Members were (and continue to be) damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

62. Plaintiff and Class Members, therefore, are entitled to compensation for their actual damages including, *inter alia*, (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (iv) anxiety and emotional distress; and (v) statutory damages of not less than $100, and not more than $1000, each, as well as attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681n(a).

COUNT II
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

63. The preceding factual statements and allegations are incorporated by reference.

64. In the alternative, and as described above, CHS negligently violated FCRA by failing to adopt and maintain procedures designed to protect and limit the dissemination of Plaintiff's and Class Members' PII/PHI for the permissible

purposes outlined by FCRA which, in turn, directly and/or proximately resulted in the theft and dissemination of Plaintiff's and Class Members' PII/PHI into the public domain. By way of example, CHS could have:

a) Conducted periodic risk assessments and gap analysis relating to privacy and information security-related policies, processes and procedures. A comprehensive risk analysis would have identified the (i) physical vulnerability of CHS's file locations, and (ii) administrative vulnerabilities associated with storing files containing patients' PII/PHI in an unsecured and unencrypted manner.

b) Developed privacy and information security related performance and activity metrics, such as the performance of ongoing compliance reviews, physical walkthroughs (roundings), hotline and complaint management—and ensure that these metrics were an integral part of CHS's corporate governance program.

c) Taken measures to monitor and secure the data servers and areas where the files containing the PII/PHI were stored, maintained, and used, or taken measures to insure that no PII/PHI was stored in unsecured, unencrypted, and/or unguarded locations.

On information and belief, CHS took none of these proactive actions to secure and protect Plaintiff's and Class Members' PII/PHI.

65. It was reasonably foreseeable that CHS's failure to implement and maintain procedures to protect and secure Plaintiff's and Class Members' PII/PHI would result in an unauthorized third party gaining access to their PII/PHI for no permissible purpose under FCRA.

66. As a direct and/or proximate result of CHS's negligent violations of FCRA, as described above, Plaintiff's and Class Members' PII/PHI was stolen and/or made accessible to unauthorized third parties in the public domain.

67. As a direct and/or proximate result of CHS's negligent violations of FCRA, as described above, Plaintiff and the Class Members were (and continue to be) damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non- economic harm.

68. Plaintiff and Class Members, therefore, are entitled to compensation for their actual damages, including, *inter alia*: (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (iv) anxiety and emotional distress; and (viii) attorneys' fees, litigation expenses and

costs, pursuant to 15 U.S.C. §1681o(a).

COUNT III
NEGLIGENCE/WANTONNESS

69. The preceding factual statements and allegations are incorporated by reference.

70. CHS had a duty to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

71. CHS negligently and/or wantonly violated its duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII/PHI (as set forth in detail above).

72. Alternatively, CHS's conduct set forth herein was so reckless and so charged with indifference to the consequences of its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' PII/PHI (as set forth above) as to amount to wantonness under Alabama law.

73. It was reasonably foreseeable that CHS's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII/PHI would result in an unauthorized third party gaining access to such information for no lawful purpose.

74. Plaintiff and the Class Members were (and continue to be) damaged as a direct and/or proximate result of CHS's failure to secure and protect their PII/PHI in the form of, *inter alia*, (i) improper disclosure of their

PII/PHI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (vi) anxiety and emotional distress— for which they are entitled to compensation.

75. CHS's wrongful actions and/or inaction (as described above) constituted negligence and/or wantonness at common law.

COUNT IV
NEGLIGENCE *PER SE*

76. The preceding factual statements and allegations are incorporated by reference.

77. Federal and state statutory law and applicable regulations, including HIPAA's Privacy Rule and Alabama state law referenced above, set forth and otherwise establish duties in the industry that were applicable to CHS and with which CHS was obligated to comply at all relevant times hereto.

78. Defendants violated these duties by failing to safeguard and protect the Plaintiff's and Class members' PII/PHI, which resulted in an unauthorized disclosure of the Plaintiff's and the Class Members' PII/PHI.

79. The purpose of HIPAA's Privacy Rule and the Alabama law cited above is to define and limit the circumstances in which the protected health information of individuals such as the Plaintiff and Class Members may be used or disclosed. The stated purpose of HIPAA's Privacy Rule was also to establish minimum standards for safeguarding the privacy of the individually identifiable health information.

80. The unauthorized disclosure of the Plaintiff's and Class Members' PII/PHI at issue in this action was exactly the type of conduct that the legislation referenced above was intended to prohibit, and the harm at issue in this case that has been suffered by the Plaintiff and Class Members is the type of harm the legislation referenced above was intended to prevent.

81. Plaintiff and Class Members fall within the class of persons HIPAA's Privacy Rule and the state law were intended to protect.

82. The harm suffered and that may be suffered in the future by the Plaintiff and Class Members is the same type of harm HIPAA's Privacy Rule and state law were intended to guard against.

83. As a direct and proximate result of CHS's violation of HIPAA's Privacy Rule and the state law referenced above, Plaintiff and Class Members were damaged in the form of, without limitation, expenses for credit monitoring and insurance, expenses for periodic credit reports, out-of-pocket expenses,

anxiety, emotional distress, loss of privacy, and other economic and noneconomic harm.

COUNT V
INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

84. The preceding factual statements and allegations are incorporated by reference.

85. CHS's failure to secure and protect Plaintiff's and Class Members' PII/PHI directly resulted in the public disclosure of such private information.

86. Dissemination of Plaintiff's and Class Members' PII/PHI is not of a legitimate public concern; publicity of their PII/PHI would be, is, and will continue to be offensive to reasonable people.

87. Plaintiff and the Class Members were (and continue to be) damaged as a direct and/or proximate result of CHS's invasion of their privacy by publicly disclosing their private facts (i.e., their PII/PHI) in the form of, *inter alia*: (i) improper disclosure of their PII/PHI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (vi)

anxiety and emotional distress— for which they are entitled to compensation. At the very least, Plaintiff and the Class Members are entitled to nominal damages.

88. CHS's wrongful actions and/or inaction (as described above) constituted (and continue to constitute) an ongoing invasion of Plaintiff's and Class Members' privacy by publicly disclosing their private facts (i.e., their PII/PHI).

COUNT V
BREACH OF EXPRESS OR IMPLIED CONTRACT

89. The preceding factual statements and allegations are incorporated by reference.

90. Defendants had a written understanding with the Plaintiff and the Class Members as set forth in CHS's Notice of Privacy Practices that CHS would not disclose Plaintiff's or the Class Members' confidential information in a manner not authorized by applicable law or industry standards.

91. CHS's Notice of Privacy Practices provided to Plaintiff and the Class Members through its hospitals constitutes an express contract or at the very least created a meeting of the minds that was inferred from the conduct of the parties. Plaintiff and the Class Members fully discharged their obligations under the contract.

92. CHS breached its contracts with Plaintiff and the Class Members by failing to safeguard and protect Plaintiff's and the Class Members' PII/PHI such

that an unauthorized disclosure of Plaintiff's and the Class Members' PII/PHI occurred.

93. As a direct and proximate result of CHS's breach of its contracts with Plaintiff and the Class Members, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

94. As further damages, Plaintiff and the Class Members request restitution and costs of mitigation including, but necessarily limited to, the purchase of credit monitoring, credit insurance, periodic credit reports and expenses associated with the loss or replacement of the valuable medical information contained in the medical records.

RELIEF REQUESTED

95. The preceding factual statements and allegations are incorporated herein by reference.

96. DAMAGES. As a direct and/or proximate result of CHS's wrongful actions and/or inaction (as described above), Plaintiff and Class Members suffered (and continue to suffer) damages in the form of, *inter alia*: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure of their PII/PHI; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (v) the value of their time spent

mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under FCRA— for which they are entitled to compensation. Plaintiff and Class Members also are entitled to recover statutory damages and/or nominal damages. Plaintiff's and Class Members' damages were foreseeable by CHS and exceed the minimum jurisdictional limits of this Court.

97. EXEMPLARY DAMAGES. Plaintiff and Class Members also are entitled to exemplary damages as punishment and to deter such wrongful conduct in the future.

98. INJUNCTIVE RELIEF. Plaintiff and Class Members also are entitled to injunctive relief in the form of, without limitation, requiring CHS to, *inter alia*, (i) immediately disclose to Plaintiff and Class Members the precise nature and extent of their PII/PHI contained within the files stolen in the Data Breach, (ii) make prompt and detailed disclosure to all past, present and future patients affected by any actual or potential data breaches of their PII/PHI, (iii) immediately secure the PII/PHI of its past, present, and future patients, (iv) implement the above-referenced proactive policies and procedures in order to secure and protect its patients' PII/PHI and be in a position to immediately notify

them about any data breaches, (v) submit to periodic compliance audits by a third party regarding the implementation of and compliance with such policies and procedures, and (vi) submit to periodic compliance audits by a third party regarding the security of its patients' PII/PHI within its possession, custody and control.

99. ATTORNEYS' FEES, LITIGATION EXPENSES AND COSTS. Plaintiff and Class Members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action pursuant to, inter alia, 15 U.S.C. §§ 1681n(a); o(a).

WHEREFORE, Plaintiff, on behalf of herself and Class Members, respectfully request that (i) CHS be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiff be designated the Class Representatives, and (iv) Plaintiff's counsel be appointed as Class Counsel. Plaintiff, on behalf of herself and Class Members, further request that upon final trial or hearing, judgment be awarded against CHS, in favor of Plaintiff and the Class Members, for:

(i) actual damages, consequential damages, FCRA statutory damages and/or nominal damages (as described above) in an amount to be determined by the trier of fact;

(ii) exemplary damages:

(iii) injunctive relief as set forth above;

(iv) pre- and post-judgment interest at the highest applicable legal rates;

(v) attorneys' fees and litigation expenses incurred through trial and any appeals;

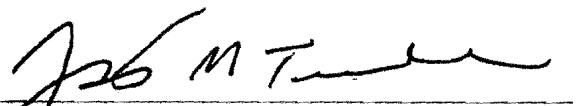
(vi) costs of suit; and

(vii) such other and further relief that this Court deems just and proper.

JURY DEMAND

Plaintiff, on behalf of herself and all others similarly situated, respectfully demand a trial by jury on all of the claims and causes of action so triable.

Respectfully submitted,



Robert G. Methvin, Jr.
James M. Terrell
McCALLUM, METHVIN & TERRELL, P.C.
2201 Arlington Avenue South
Birmingham, AL 35205
Tel: (205) 939-0199
Fax: (205)939-0399
Email: rgm@mmlaw.net
Email: jterrell@mmlaw.net
Attorneys for Plaintiff

OF COUNSEL:
M. Adam Jones (ASB-7342-J63M)
Jordan S. Davis (ASB-5103-D58D)
M. ADAM JONES & ASSOCIATES, LLC
206 N. Lena St.
Dothan, AL 36303-4429
Tel: 334.699.5599
Fax: 334.699.5588
Email: Adam@AdamJonesLaw.com
Email: Jordan@AdamJonesLaw.com

PLEASE SERVE THE FOLLOWING DEFENDANTS BY CERTIFIED MAIL:

Community Health Systems, Inc.
4000 Meridian Blvd
Franklin, TN 37067

Community Health Systems Professional Services Corporation
4000 Meridian Blvd
Franklin, TN 37067

Triad of Alabama, LLC d/b/a Flowers Hospital
c/o Corporation Service Company
150 South Perry Street
Montgomery, AL 36104